
Exploring *Second Life*

Interview with Cory Ondrejka

Interviewed by John Whisenhunt, Editor

Editorial Abstract: *Mr. Cory Ondrejka, Chief Technical Officer of Linden Lab, was a guest contributor at the “Discrediting Suicide Bombing: An Information Strategy” seminar. He explains the challenges of operating a large scale, open source cyber environment, and how similar constructs might help serve US and Coalition influence efforts.*

IO Sphere: *In the influence business, we’re always trying to find people who can work “both sides of the brain.” You and your current efforts represent that sort of ability, yet the path from Navy engineer to the cyber world seems unusual. Can you talk about this evolution?*

CO: <laughs> You don’t see that as a completely normal path?

IO Sphere: *Well, in the influence business we seem to have folks that are definitely more one side than the other! Some certainly would view it as normal.*

CO: I left the Navy during the 1990s drawdown at the end of the Cold War, when we had less need for submarine warfare officers, then went to work for Lockheed. I was doing some electronic warfare work which we still can’t talk about, which was very challenging, requiring unconventional thinking. We were going from custom hardware to commercial off-the-shelf, the transition from VMX to UNIX—which were large changes in the Defense community, as we were maybe half a decade to a decade behind the civilian world. The catch up took a lot of education, and some trade-offs—it was more than just developing new hardware, we were also able to significantly increase capabilities and hire people more easily to work on this stuff. Then in 1995, a friend asked me to come to California to help start an electronic games company. This was at the tail end of the arcade era, the old “pump in quarters” model. But the interesting thing was that we were designing hardware and software at the same time—very challenging—but



Cory Ondrejka (Linden Lab)

you’re also building a game on top of that. We had to capture someone’s imagination in 45 seconds, from something they may never have seen before, and make them want to play again. That’s a pretty strict set of requirements when also writing software and developing hardware. So I did that for a couple of years, and then some console game development, then Philip Rosedale, founder of Linden Lab, and a buddy of his had been mucking about a couple of years working interfaces and compression technology, and he had these great big ideas. We met sort of randomly, but had a big six hour conversation, and at the end it was “when do you want to start?” So it was come on in, build the team, architect the system, and try to build something with very little idea of how you would do it. So a large part of my career has been trying to do something that has never been done before—find a set of challenges that don’t have known

solutions and go try and solve them. This is what’s made Linden Lab very easy to hire for, because we offer the most interesting set of technical challenges, plus learning opportunities: come learn about intellectual property law, come learn about learning theory, or about cognitive science. You need to know about these things to build something like *Second Life*. So, in hindsight I see all this as a very logical progression <laughs>, though examining it in the Lab some might see it as a major step function difference—though it’s been much smoother than that!

IO Sphere: *If we’re looking to cultivate similar problem-solvers for government and industry, what path would you recommend to someone who wants to “grow up to be like you?”*

CO: Let me answer the first part, because I’m not sure about growing up to be like me! We think about problems, and none of them exist purely in one side of the brain, to use your pop psychology analogy. If you’re an academic it’s qualitative versus quantitative. The world is full of false dichotomies that simplify our thinking when we look at highly-stovepiped, highly-specialized organizations—plus things like the sound bite—to simplify highly complex ideas and challenges. The danger is relying too much on the simplification, because you begin to think of it as the problem. For example, in the nuclear Navy, one of the first things that gets beaten into your head is you never, ever use an acronym! Which is funny, because it’s the military. So you ask, why is that? I mean, you read any documentation and it’s full of acronyms. The danger is if you use the acronym then you might forget

what it really means—the risk of losing understanding—and building habits that are not the right habits. This is the legacy of [Admiral Hyman] Rickover, and why we don't automate a great deal of nuclear Navy reactor operations, because people in-the-loop are better. We catch mistakes better than a lot of other systems, if we're vigilant all the time. If you're the young officer first learning to run a reactor, the petty officer turns to you and says "Sir, are you absolutely sure you really want to be doing that?" So, we assume everybody is about to make a mistake. It doesn't mean they're not smart, nor as capable as you or anyone else, but double-check everything! To me it was very much a formative experience. Now you carry that into what I do today, but with my electrical engineering degree, a computer science degree, graduate work in nuclear physics—so a lot of science and engineering background—which is very much the classic method: look at the results, don't trust hearsay or anecdotal evidence, and verify, verify, verify! Now at the same time, I've spent a lot of time building products for entertaining people, trying to capture their attention, and when you start doing all of that, you start recognizing how really important both pieces are. It's like talking to qualitative versus quantitative academics who both view this as a big breach: the quantitative people mock the qualitative people as being 'fuzzy,' and the qualitative people mock the quantitative types as just 'not getting it.' But when you look at when science really moves forward, it's always a combination of both. My favorite study that illustrates this is a US FDA [Food and Drug Administration] metastudy on studies of drug efficacy. What they looked at was the funding source. Turns out, if your funding source was the creator of the drug, your study come out twenty to forty percent more in favor of the drug. Now you'd say that's what we suspect; from a qualitative standpoint this suspicion is probably what triggered the study. But then we got a quantitative answer. This is when science is at its best, when engineering is at its best: you use procedures and methods, but are always examining and re-examining them.

So when it comes to building something like *Second Life*, which is something that had never been successfully built before—the idea of building a collaborative virtual space that wasn't a game—it was a tremendous engineering challenge. From a data compression standpoint, a distributed computing standpoint, networking, rendering... but there's a whole other piece of it. How do you bring people into a world where you can do anything? There aren't the clear goals a game provides, or the simplifying functions a game provides. So when we look at similar challenges around the world, we see a similar set of practical pieces: it's just a non-starter if you can't communicate, gather information, or share it. But until you know the right questions to ask, you're not putting the right information in, and we're back to the classic computer science axiom of 'garbage in, garbage out.' So when we look at how we'll be training people for this, and preparing them, they'll want challenges like this. Engineers and nuke geeks like me don't want to learn the fuzzy stuff—what need is there? But on the flipside, you have people saying "why would I want to learn statistics?" Both of those are very dangerous positions to take because you're cutting out an enormous set of tools.

So when we face things like cross-cultural understanding, and extremism, none of the solutions is going to be in one realm or the other. The classic example for intercultural dialog turns out to be music. Everyone likes to listen, and many enjoy music from far off in another part of the world. If you're a 'real' music person, you like the new stuff, because that's what's cool. And that's a huge technology problem. How do you get a musician sitting on the street in Baghdad on the Internet? How do you share his music, and how do you get money back to him to say 'thank you?' Could you create a fan base for him? Could you have him collaborate with a musician in Germany or Brazil, or the US? There are technology layers to enable all that, but all of these are social questions, diplomacy questions, cognitive questions. So, how do we foster and leverage all that? These

are all very worthy of taking on, and once you realize how interesting these challenges are in the space that intersects the cognitive sciences and sociology and anthropology, then it's easy to get motivated and draw people in!

***IO Sphere:** You mentioned cultural expansion. You have global presence with *Second Life*, and have responded to recent press reports of the US's adversaries using your environment. Where might all this be going? Do you expect to have a server farm in places like Riyadh someday?*

CO: There area host of questions there. There is a lack of clarity about exactly who is using various forms of technology, from *Google Earth*, to *Second Life*, to the Web as a whole. We all want to learn more about what's happening in that space. Next, if you look at some of the research being done at USC [University of Southern California] and the Annenberg Center [USC School of Communications] about what happens when you bring people of different cultures together, and have them engage in goal-oriented behavior, you start seeing opinion changes that look a lot like exchange programs. Which is very interesting, because it's a lot safer to move bits around than people. So what are we lacking there, and what opportunities are we not yet taking advantage of yet? Another question is what opportunities does technology give us? Something I've heard time and time again from the [US] State Department and others is that the cohort most difficult to reach in the Islamic world is women. What's interesting about that is data coming out of the Gulf region that in math, science and engineering, these are some of the highest performers. So you can't reach your most educated cohort, and they're unemployed. It sure seems like technology should be able to help us there. How do you reach them, and give them a way to reach each other? Can they hold jobs and lead via the virtual community? These are questions we're just starting to ask. What's so exciting is when I look at a set of people I've worked with—the virtual world, games,

entertainment—what I’ve heard people saying the past five years is “how do I pivot my career a little bit to help make the world better? How do I help?” They may not have forty hours a week to do that, but they may have five, or a few hours a month. The great potential for the Internet or *Second Life* is to enable more diffuse groups to still be productive and effect change. It’s a technology question, but is far more social and economic in scope. This morning we heard about how a large cohort of extremist recruitment comes from those ‘without hope.’ With fifty percent of the Islamic world under the age of twenty-five—a tremendous youth bulge—how do we give that group hope? Hope can be a socio-economic phenomenon: it’s a lot easier to have it when you can feed your family, be better off than your parents—when you have some control over your future. In an age when we can do education and work at a distance, and call centers all over India... what analog can we use to take technology into these economically struggling regions? So to the question of who’s using this, about seventy percent of *Second Life* is international: the US is the minority of total users. Because there isn’t a lot of broadband penetration in the Gulf region, that’s still not a big *Second Life* user area—but it’s growing. I think what we’re going to see there is the real opportunity to use the virtual world as a vector for education, business, collaboration, for culture, music... for sharing and remixing. All of that is going to be exciting to watch.

IO Sphere: *We’ve already touched on part of this, but can an evolution of something like Second Life provide a training ground for countering extremism?*

CO: I think the key there is how we allow technology to let them be their own voice against extremism. It was interesting to hear people talk this morning about how some Web groups are already discrediting extremism and violence: terrorists, suicide bombers and the like. This was followed by how do we [the West] want to message this? There’s a contradiction there! If the community



(Copyright 2007, Linden Research, Inc. All Rights Reserved)

itself is already discrediting some of this, then having an external voice attempt to support that can be counterproductive. The nice thing about Web environments and *Second Life* are that they are exactly what the users want them to be. So as a place for mothers to create discussion for a better future, where their children are safe, and for young students to talk about brighter futures, or to start designing what structure they’ll rebuild first... or how to be entrepreneurs and business people... absolutely the technology can be used for this! The ways to foster this are not to message at them, but instead to say how do we make the technology and the broadband access available? Are there computers and cell phones and seed funding available for entrepreneurial activities? I bet US \$5000 gets you a pretty good business opportunity. Obviously we can’t do that where you don’t have safety and security. But working online also gives you pseudonymity, so you can work in a way that even if an extremist doesn’t like what you’re doing, if they can’t determine your real world identity, you have some measure of protection you wouldn’t have in the real world. So from a security standpoint there may be other reasons we should start pushing in that direction.

IO Sphere: *You mentioned protection of this ‘freewheeling’ sophisticated cyber environment. You’re bringing all sorts of behaviors and potential hazards into the virtual world. Cyber law is still*

evolving. Don’t you have to bring laws with you? How do you police it?

CO: It’s an excellent question, but be careful about getting swept up in the metaphor. Ultimately this is bits sitting on servers, moving through the Internet, and being rendered on individuals’ machines. This is the World Wide Web we know. There is already a body of cyber law to cover these things. This is not to say, as you alluded to, that cyber law is complete or consistent, but there is a real danger in getting too wrapped up in the metaphor: all the people involved and all the servers still exist in the real world. If you break a law using *Second Life*, you’re still breaking the law in the real world. Like the Web, it took a while for law enforcement and regulators to recognize that all the computers are still in the real world—yes there are additional complexities because you get into multi-national and multi-jurisdictional areas—which does raise rather interesting questions. You have all the places in the world where YouTube is banned right now because of content. But the scary part is you start getting into an information regulation ‘arms race.’ If your only approach is dealing with information you don’t like is to attempt to cut it off, you’re missing the chance to use the same technology to get your message out. Ancient cultures with real messages of their own could be sharing, could be using the same technologies to block what they consider cultural infringement. Instead, they chose to ‘pull the plug.’ Look at what will pull a nation’s economy into the new century, and cutting things off is not a good step. So this becomes the arms race. There are a lot of good ways to move data around, so you either hire a million censors—the Chinese model—or you pull the plug. Neither of these are a good economic move, or provide your population with tools they need to join the new economy. Now let’s not overhype, as in ‘the Web changes everything’—but it really has changed things: there is more information all over than planet than any time in history. It’s cheaper to find things, the cost of learning is lower, innovation is higher...

but we're hardly done yet! If you pull the plug, you guarantee you'll miss a lot of the good stuff. Because innovation is an exponential, you'll be well behind that curve in fifty years. Mexico and Singapore had comparable economies thirty years ago, and they don't today. Certain investments in education and infrastructure pay off very well.

IO Sphere: *Let's talk about something of interest to our network defenders. As a CTO you have a huge infrastructure and a large open source community. How do you deal with risks?*

CO: Let me clarify your question. Are you equating open source with security risk? I would argue strenuously the opposite is true!

IO Sphere: *People unfamiliar with the open source community might think that many creative people could introduce something you don't want.*

CO: This goes back to the information governance question. You can never fully rely on 'security through obscurity'—we know that. Whatever security you're looking at, be it cyber or for that matter a convoy in Iraq, you've got a massively distributed opponent using a distributed assault on the design space: which is find weakness—local minima—and exploit them. Once exploited, they share it with everyone else until that local minima is closed. Centralized ways of countering decentralized attacks are very rarely effective and they are always expensive. So for us with the client—*Second Life's* open source part—there was a very active reverse engineering effort, and they were starting to expose bugs. Every popular piece of software has this going on. Once you have something on your computer, you can figure out what it does—you don't need the code. But if they don't have the code, they can't help you fix the bugs, right? If you don't go open source, you have the worst of both worlds because they'll still reverse engineer your product, but they can't help you!



An outdoor classroom in the Second Life world. (Copyright 2007, Linden Research, Inc. All Rights Reserved)

Certainly security is never a singular piece: it is a global problem with human, electronic, and social components. So when you think about any product or service you're using: where are your vulnerabilities? You have to think "can user creation help or hurt you?" For *Second Life*, there is no question that by giving our users a fully-featured scripting language they can attack the system from within and try to consume all the system resources or crash the grid. Right now there are twenty million 'hostile' scripts—meaning I didn't write them—being executed on the *Second Life* grid. This is very much a 'Holy Grail' problem in computer science, accomplishing what we have already accomplished. Our users generate three hundred gigabytes of user data per day, and twenty million lines of code a week, so that's the trade off. So what did we do? We built a system where they could do anything they wanted within that scripting language, but it wouldn't take down the system—or if it did, it would be localized or encapsulated so we could deal with it. For us, that was the right decision. It that right for everything? No. Look at the Web. It would not be what it is today if we had some guy sitting in an office who you submit your Web page to for approval, for justification of your own creativity.

We wouldn't have the Web. No one is arguing the Web should have grown in a centralized way.

So what do you want out of what you're building? Some of what we've talked about today in the seminar on dealing with other cultures brings up some deep questions. Any message that comes from the US to the Islamic world is immediately discredited because of where it originated—end of story—doesn't matter the value. I think we can see where they're coming from. So how do we work around that? You could roll out technology to let them talk to one another, or public discourse among civil society, where you're only one voice of many. There's been some discussion on this, like the Open Source Intelligence Initiative, and get analysts in on the public discussions—you've got Web anonymity. Or you could say "I'm just an analyst trying to learn about your culture." So there are trade-offs, and it comes from understanding the problem and not being dogmatic about any piece of it. If we go in saying "we'll never open source that," or "we'll never do that transparently," well, that's a dumb starting point. Dogmatic positions aren't always right. At Linden Lab, we constantly try and remind ourselves we can't be dogmatic about anything. We're a radically decentralized product

created by a very decentralized internal organization. But once we grew past 200 people, we're having the discussion of where we need a little more organization and information flow hierarchy, so people aren't buried in many-to-many communications. Always question, and in a way that keeps you from being personally affected, so you can ask the really difficult questions. This is where insisting on data, and insisting on challenging assumptions can be so useful. Otherwise you get into the "but that's my baby" situations. One decision I made early on at Linden Lab was that no developer 'owned' a piece of code. Only slightly tongue-in-cheek I told the team "if I ever hear you say 'don't touch that, it's my code,' I'm going to fire you!" It turns out our developers are happy working in that environment, as I found out building previous smaller teams, but it's the opposite of how most software companies organize. We don't bind projects to offices or geography, but to the right people to work them. You may be working with the guy right next to you this week, but a guy in England the next. You pick up a little extra cost and communications overhead, the positives are the right bodies on the job, and move away from people arguing that "this is my code, and only I can do it the right way." As opposed to "dude, this was great two years ago, but we need to toss it and write something better." That was tough, as much of the original *Second Life* code was mine! But you have to evolve. But can we find exactly that sort of attitude other places, of course. So you need to be dogmatic about not accepting dogma! So I'd say, you simply have to be transparent.

IO Sphere: *That kind of leads us into the last question. The federal government has some pretty fierce dogma, and doesn't change easily, so how do you suggest we help crack that?*

CO: Let's look at how *Second Life*'s philosophy tends to be adopted at other larger organizations. Or, let's drop back one and talk about how the Web was adopted. Option A: guy at the top/CEO

says "we will use technology A," i.e. "all government software code will be written in Ada [programming language]," and we know how spectacularly well that worked! Option B: folks at the edges say "I found this thing, and it's useful." Then before you know it, "well this email thing is kind of useful," and "hey, I'm capturing our internal procedures on a wiki, so if you find a mistake you can just fix it." That's what happened during the late 1990s: the Web came in, was bottoms-up adopted, and big companies like IBM validated it, and created some enterprise products. So when the top down direction came, the grass roots support was already there because people on the edges had been using the Web at home, and as much as possible at work. So when it comes to *Second Life*, it's quite similar: one day people notice their employees are using it. They're not using it for shopping, but for meetings among groups that are physically far away from one another, for brainstorming, for prototyping. When you're attempting to change large centralized organizations, viral and bottoms-up methods are very useful, because they're self-validating. When somebody decides to go through the effort, they're doing so because it makes their lives easier, not because Mr. CEO said "you better use this or I'll fire you!"

So for the US Government, we're already seeing say a dozen organizations, experimenting with *Second Life* to varying degrees—very much in bottoms-up way. If it doesn't work for your organization, wait six months... just like the Web. Hey, this blogging thing came along, and it's helpful for us. A second thought is Craig Newmark, who founded Craig's List. He talks about the Web being a big force multiplier for the individual: you don't need the same capital expenses; you don't need the same resources to be very big. *Second Life* is like that even more so, because the design space we offer is much larger. So the US Government says, "We're just not comfortable with being transparent about certain things." Innovation and security have also been at odds, just like science and security—the dynamic tension says

there are some understood trade-offs. But, if we could just get these two groups talking, we'd see some innovation, but we're uncomfortable with it, and with the security implications. But the default for secrecy is always to be more secret. Policies that force you to defend secrecy are probably a good idea. For instance, at Navy nuke power school our course books were classified, and the Pythagorean Theorem as far as I know has never been secret! But it forced us to treat all our books the same, and that's a defensible reason, but make sure you have that discussion ahead of time! But was the math curriculum as good as it could have been? We couldn't share it with say, Princeton [University], and say "how does this compare?" So, it's surfacing the trade-offs and making those transparent. Perhaps if you don't share the actual data, you can still make your decision process transparent, and people aren't thinking you're keeping a secret just to keep a secret. But the other option is if the US Government isn't ready to implement thus, maybe you can seed other people to go try. There are some really interesting questions, such as should public diplomacy even be a government function? Public diplomacy is starting to get a very bad name because it's turned into selling politics, which isn't what it always was. Historically it was intermingling of cultures, and both came away liking and understanding each other more. That's not hard to imagine, because people tend to like other individuals. They can figure out all kinds of reasons they don't like groups, but individuals together and you can change their opinions about the group.

IO Sphere: *Which is why exchange programs tend to work so well.*

CO: Exactly right. So why not fund non-governmental exchange programs, and technologies that do similar things? If the government is uncomfortable, then just fund a few thousand or a million dollars—or pick a number—and fund say, ten ideas. Then measure them, see how well they do. That's pretty easy, and the Web and virtual space give you a great force multiplier than thinking

about this in terms of America's Houses, or exchange tours or visa programs. These are tough because you're moving people. And that's incredibly expensive, and a risky prospect: it's dangerous to move people these days. Instead, let's have the government do what it's good at, and if they figure out something they're not good at—then don't do it. Let someone else do it, and learn from them. Get better at it slowly, and don't get hamstrung, or get hung up in local minima.

Let's say we want to create a network to talk about extremists, and the government says we're not comfortable with that, so let's put State Department branding all over it, only accessible from government sites—and that defeats the entire purpose! And you spend money doing it, it's declared a failure. I'm not saying the government would do that, but it will make it that much harder to adopt these ideas at a time when extremist groups of all flavors are using them today. If you want to be appropriately terrified, look at their cartoons and games... pick your extremist group. And those same things are being used by white supremacists, violent anti-abortion groups and the like. Fringe groups tend to move to fringe communication media, and that dates back to the printing press. Why? Because hopefully nobody notices you there. So the idea of not using these same media forms in positive ways seems like a tremendous lost opportunity—and could be disastrous.

Another thing we saw this morning was the proposal for us [the West] to influence Islamic blogs. In the marketing world that's called 'astroturfing,' literally attempting to generate a 'fake grass roots' movement. And you know what? Astroturfing campaigns are always discovered... always, always, always! Because communities are very well inoculated against outsiders—very good at detecting 'that which is other.' Guess what happens when astroturfing gets discovered: the company that did it is vilified in the blogs they were trying to positively influence... and that loss of influence is almost immeasurable! So guess what will happen if we try and

do that? If the message is hypocritical, or something that isn't true, you'll get discovered, and both sides will have a tremendously adverse reaction. That's why doing this in some sort of centralized [government] way is going to be very, very tricky – potentially very dangerous. Imagine if we create a blog and say "Iraqis, go use this to talk about anti-extremism." Then, I pretty much guarantee someone will use it to plan a suicide bombing, and then the headlines read "US Government creates network to allow suicide bombing attempt!" Which means we have to be ready for that, and say "here are the thousand success stories." But that's a difficult position to be in, especially if you're actually operating the site, so a layer of indirection might be very helpful in getting people to use the site as well as better manage it. Communication media is going to get used in other ways... well, you can detect that and help steer it. But look at the problems *MySpace* is having: they are scanning more, and hoping to look for more problems, and sharing data when subpoenaed. Law enforcement has practices for dealing with these things, but you have to be ready for that. So from a US government perspective, you have to look at the positives coming out of this, and recognize this is a learning

process—we're not always going to be right, but it's not like we've been right to date in this effort. We've made some tragic mistakes, and losses of life are horrible. These are not simple problems, and we would have pushed the 'magic button' if such existed. This is a years-long, multi-generational effort. Look back to the unrest of the 1960s: we certainly didn't have domestic tranquility and safety in this country overnight, and we had tremendous violence along the way. Or look at our discussion in the seminar about how long progress took in Northern Ireland.

IO Sphere: We ask countries to reform their economy, build a government, and promote social programs... all at once.

CO: And respond to massive external influences, get back into the petroleum economy... it's a huge thing to ask.

IO Sphere: As much as I'd like to monopolize your time, you have more to contribute, so let's get you back in there.

CO: Thank you, I've enjoyed talking with you. 